REMARKS/ARGUMENTS

The Examiner's Action mailed on September 14, 2006 has been received and its contents have been carefully considered.

5

Applicants have amended claims 1, 2, 4-7, 10-12, 14 and 15 according to the specification and figures to overcome the rejections. Claims 1, 6, and 10 are the independent claims. Claims 1-15 are now pending in the application. For at least the following reasons, it is submitted that this application is in condition for allowance.

10

Response to Claim Rejections - 35 USC §101:

Claims 1 and 10-11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

15

According to paragraph [0051] in the specification, it is suggested that the combinatorial logic contain logic circuits, and an example of a logic circuit is illustrated in Fig.3. In order to place claims 1 and 10-11 in condition of allowance, **combinatorial logic** are specified as **combinatorial logic circuits** in the claims to overcome the

20 rejections.

Response to Claim Rejections - 35 USC §112:

Claims 1-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite

25 for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicants have indicated that their invention is for calculating a TKIP Sbox value

as required in the TKIP Sbox function, hence, reference to the IEEE specification in the claims are deleted to clarify the indefiniteness of the case when the IEEE specification modifies or evolves over time, and should now be able to particularly point out and distinctly claim the subject matter in which the Applicants regard as the invention in

5   claims 1-15.

Response to Claim Rejections - 35 USC §102:

Claims 1-15 are rejected under 35 U.S.C. 102(a) as being anticipated by Tom St.

10   Denis "Analysis of TKIP Temporal Key Integrity Protocol (hereafter "Denis").

Regarding claims 1, 6 and 11, the Examiner alleges that Denis disclosed a first plurality of combinatorial logic for calculating a TKIP Sbox left value according to a low part of an index value (Denis, pages 4-5 sections 3 and 3.1, Figure 3, x0), a second

15   plurality of combinatorial logic for calculating a TKIP Sbox right value according to a high part of the index value (Denis, pages 4-5 sections 3 and 3.1, Figure 3, x1), and a third plurality of combinatorial logic for calculating a TKIP Sbox value according to TKIP Sbox left value and the TKIP Sbox right value (Denis, pages 4-5 sections 3 and 3.1, Figure 3).

20

As could be read in section 3 of Denis, "[T]he TKIP Sbox (TS) is a 16x16 function made from the two smaller 8x8 functions.   The input is first split into two 8-bit words x1 and x0 where x0 is the least significant word of the input.   **Each of the smaller words [is] passed through the 8x8 tables TSU and TSL to form a 16-bit partial**.   After the

25   substitution the two 16-bit partials are then XOR'ed together to form the output."   It is clearly expressed in the line in bold that combinatorial logic is not applied to the smaller words (x1 and x0), whereas Denis actually applies the exact procedures as portrayed in the description of the prior art in the specification of this invention as disclosed in

paragraphs [0032] to [0039]. By making use of tables TSU and TSL where **TSU represents the table of the matrix "unsigned int Tkip_Sbox_Upper[256]" and TSL represents the table of the matrix "unsigned int Tkip_Sbox_Lower[256]"**, the TKIP Sbox left value and the TKIP Sbox right value are indexed through table lookups.
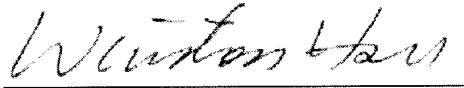
5

As mentioned in the description of the prior art in the specification of this invention, lookup tables require mask ROMs which are physically large in size, and the combinatorial logic that calculates the TKIP Sbox left value and the TKIP Sbox right value directly without the lookup tables TSU and TSL are implemented to reduce overall
10   chip space of the design. Such improvements should not be anticipated by the disclosure of Denis, thereby Applicants believe that the amended claims 1, 6, 11 are in the condition of allowance.

Similar arguments discussed above should also apply to claim 10, and if the
15   independent claims 1, 6 and 10 are found to be allowable, the dependent claims 2-5, 7-9 and 11-15 should also be allowed. For the above reasons, consideration of the pending claims 1-15 is respectfully requested.

Sincerely yours,

<u>/Winston Hsu/</u>   Date: <u>03/14/2007</u>

Winston Hsu, Patent Agent No. 41,526

5   P.O. BOX 506, Merrifield, VA 22116, U.S.A.

Voice Mail: 302-729-1562

Facsimile: 806-498-6673

e-mail : winstonhsu@naipo.com

10   Note: Please leave a message in my voice mail if you need to talk to me. (The time in D.C. is 12 hours behind the Taiwan time, i.e. 9 AM in D.C. = 9 PM in Taiwan.)